Enterprise Network Security

Accessing the WAN – Chapter 4

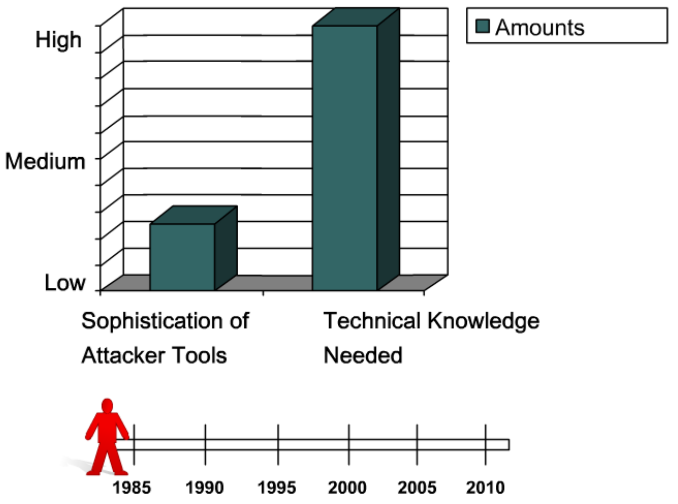
Objectives

- Describe the general methods used to mitigate security threats to Enterprise networks
- Configure Basic Router Security
- Explain how to disable unused Cisco router network services and interfaces
- Explain how to use Cisco SDM
- Manage Cisco IOS devices

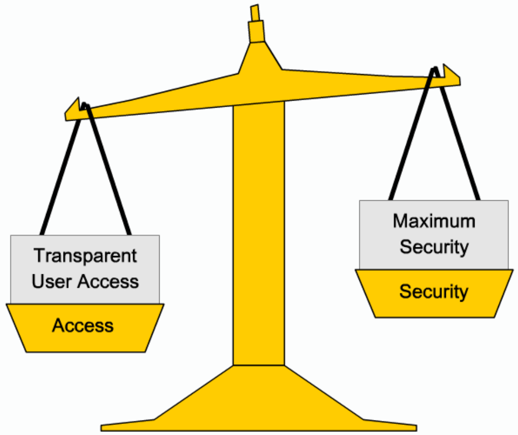
Describe the General Methods used to Mitigate Security Threats to Enterprise Networks

- Explain how sophisticated attack tools and open networks have created an increased need for network security and dynamic security policies

The Increasing Threat of Attackers



Closed versus Open Networks

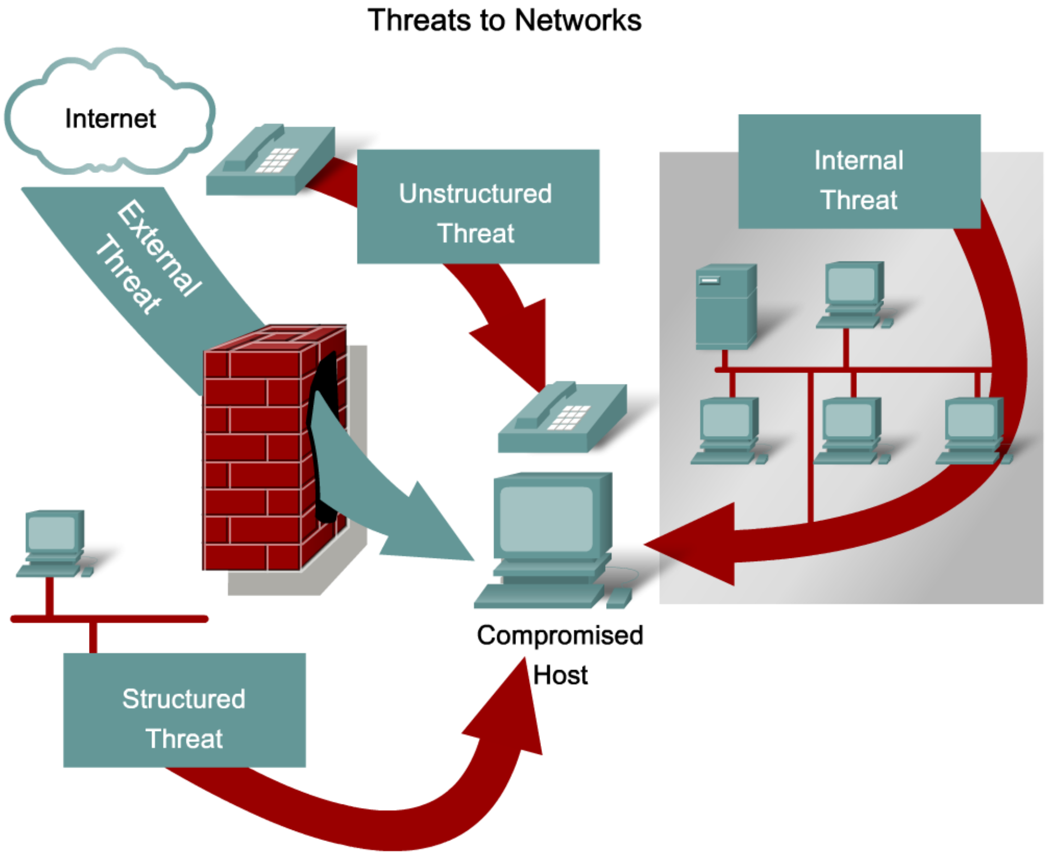


Permit everything that is not explicitly denied:

- Easy to configure and administer
- Easy for end users to access network resources
- Security costs: least expensive

Describe the General Methods used to Mitigate Security Threats to Enterprise Networks

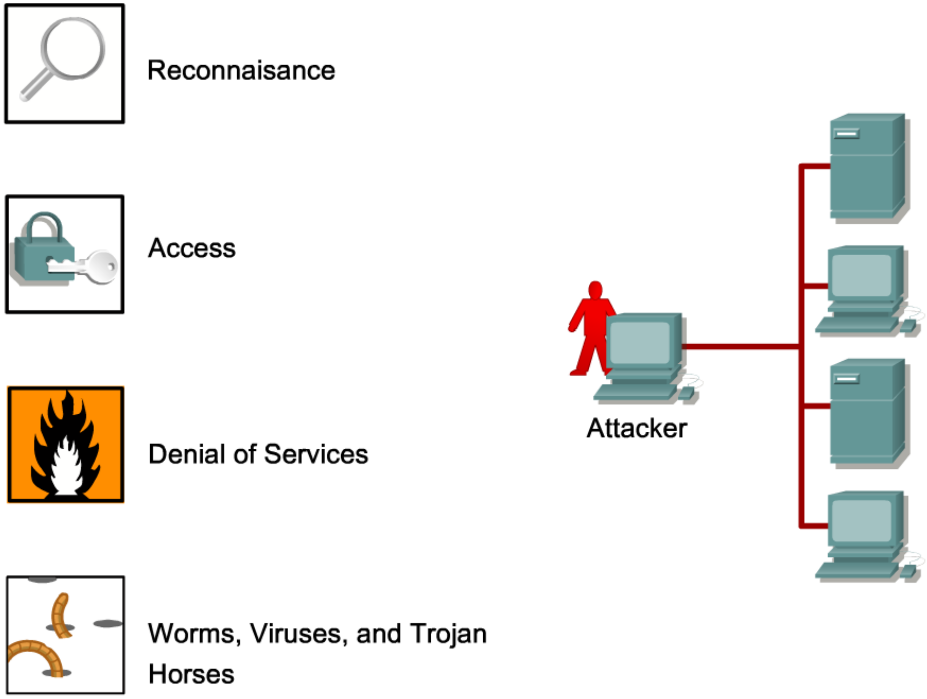
- Describe the most common security threats and how they impact enterprises



Describe the General Methods used to Mitigate Security Threats to Enterprise Networks

- Describe the most common types of network attacks and how they impact enterprises

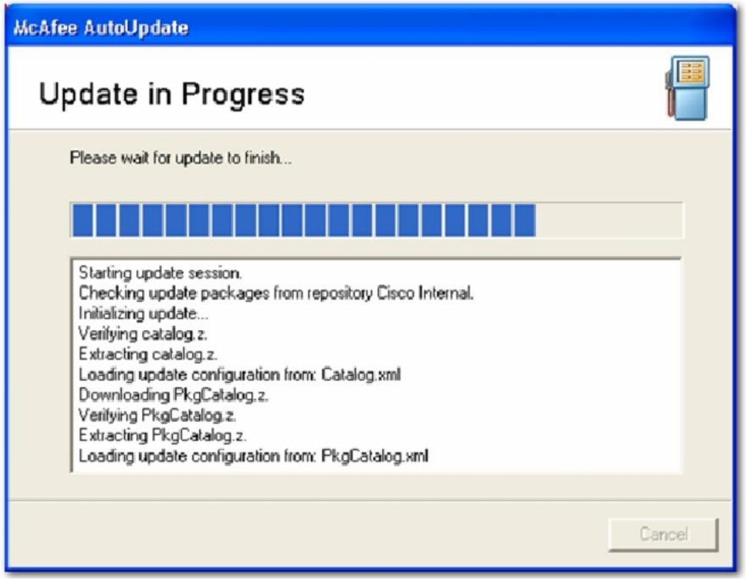
Types of Network Attacks



Describe the General Methods used to Mitigate Security Threats to Enterprise Networks

- Describe the common mitigation techniques that enterprises use to protect themselves against threats

Update Antivirus Software

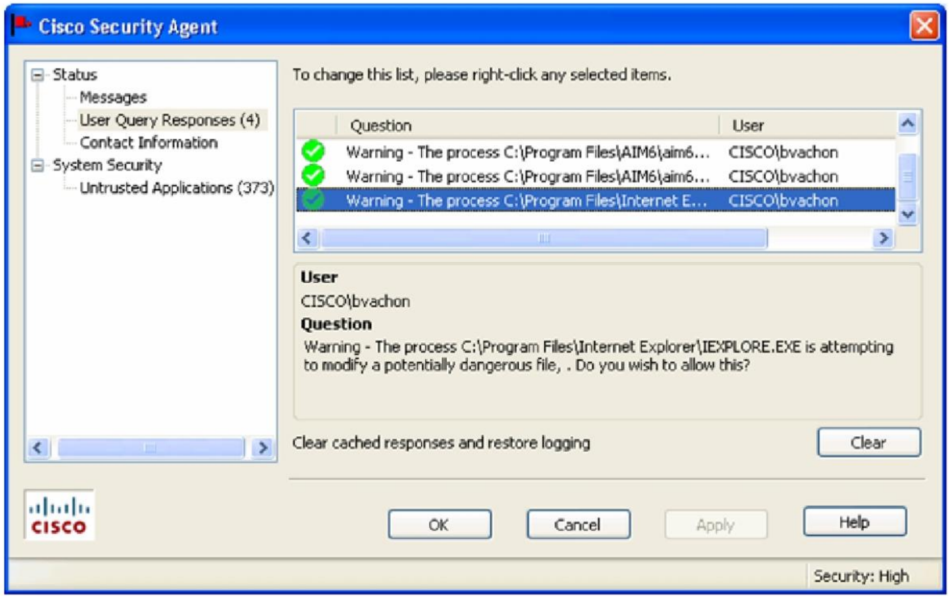


Update in Progress

Please wait for update to finish...

```
Starting update session.
Checking update packages from repository Cisco Internal.
Initializing update...
Verifying catalog.z.
Extracting catalog.z.
Loading update configuration from: Catalog.xml
Downloading PkgCatalog.z.
Verifying PkgCatalog.z.
Extracting PkgCatalog.z.
Loading update configuration from: PkgCatalog.xml
```

Intrusion Detection and Prevention



To change this list, please right-click any selected items.

Question	User
✓ Warning - The process C:\Program Files\AIM6\aim6...	CISCO\bvachon
✓ Warning - The process C:\Program Files\AIM6\aim6...	CISCO\bvachon
✓ Warning - The process C:\Program Files\Internet E...	CISCO\bvachon

User

CISCO\bvachon

Question

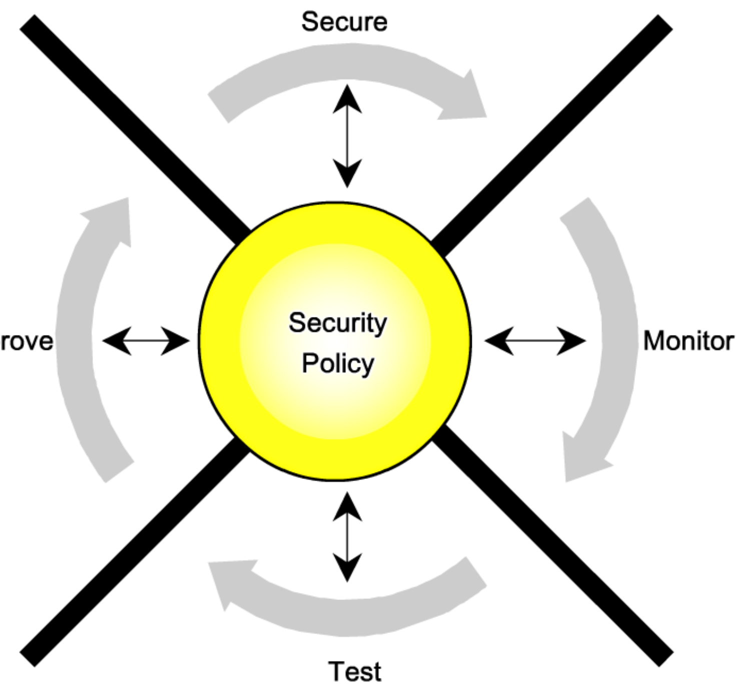
Warning - The process C:\Program Files\Internet Explorer\IEXPLORE.EXE is attempting to modify a potentially dangerous file, . Do you wish to allow this?

Clear cached responses and restore logging

Describe the General Methods used to Mitigate Security Threats to Enterprise Networks

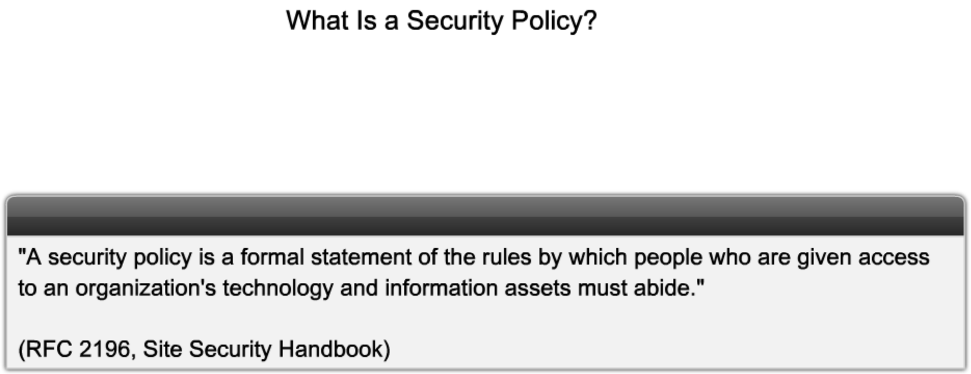
- Explain the concept of the Network Security Wheel

Network Security Wheel



Describe the General Methods used to Mitigate Security Threats to Enterprise Networks

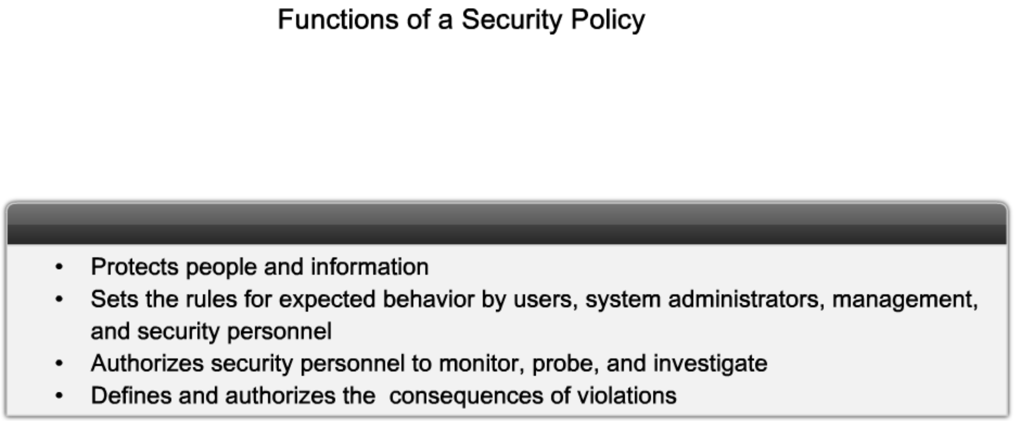
- Explain the goals of a comprehensive security policy in an organization



What Is a Security Policy?

"A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."

(RFC 2196, Site Security Handbook)



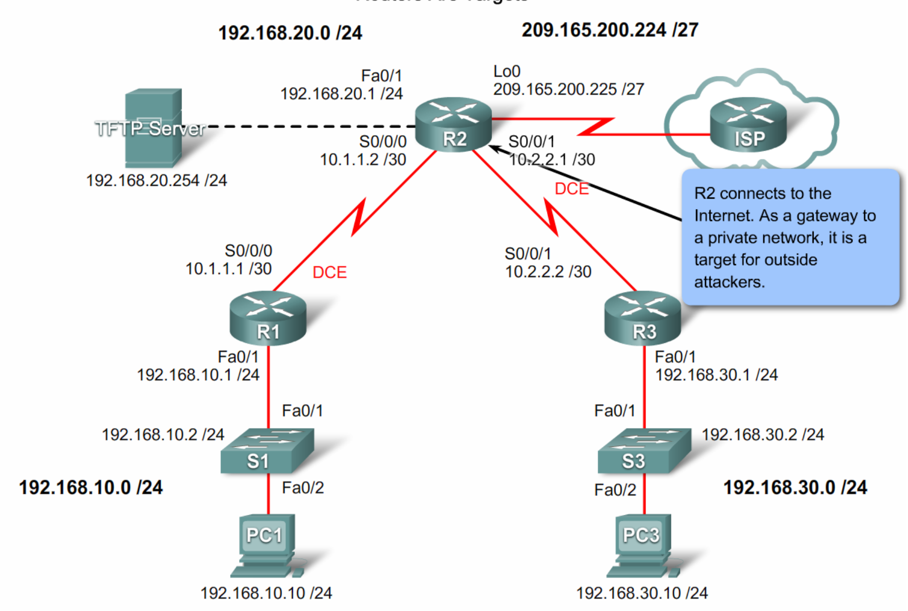
Functions of a Security Policy

- Protects people and information
- Sets the rules for expected behavior by users, system administrators, management, and security personnel
- Authorizes security personnel to monitor, probe, and investigate
- Defines and authorizes the consequences of violations

Configure Basic Router Security

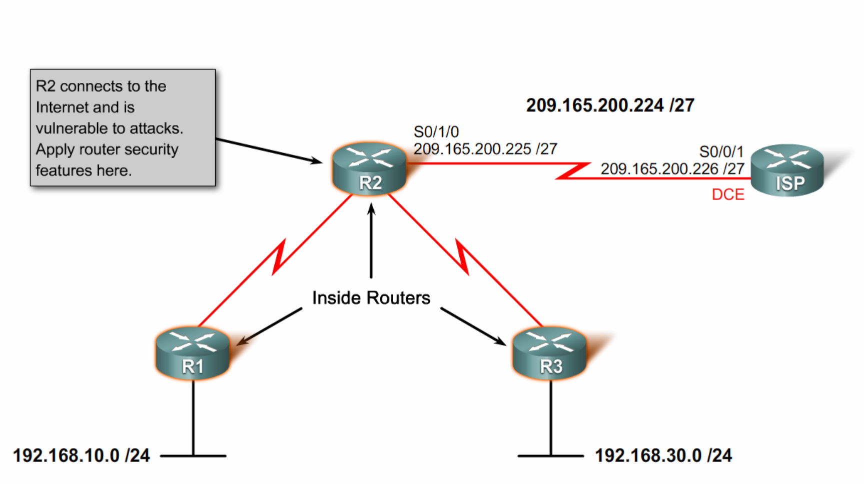
- Explain why the security of routers and their configuration settings is vital to network operation

Routers Are Targets



R2 connects to the Internet. As a gateway to a private network, it is a target for outside attackers.

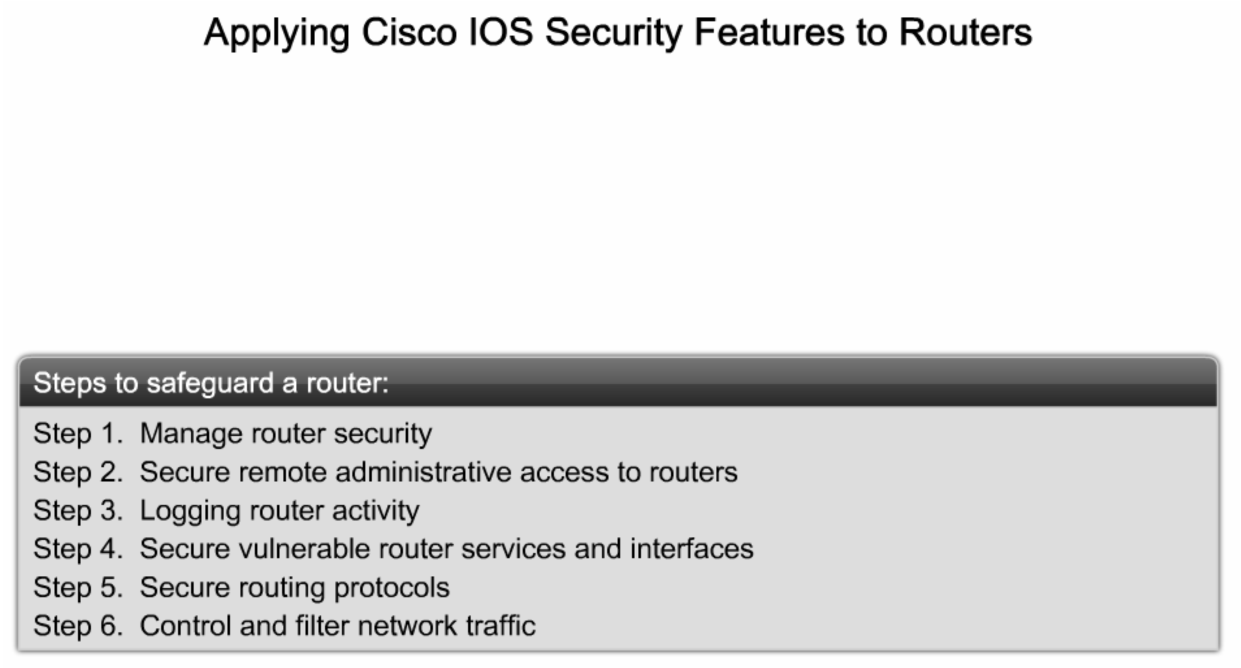
Securing Your Network



R2 connects to the Internet and is vulnerable to attacks. Apply router security features here.

Configure Basic Router Security

- Describe the recommended approach to applying Cisco IOS security features on network routers



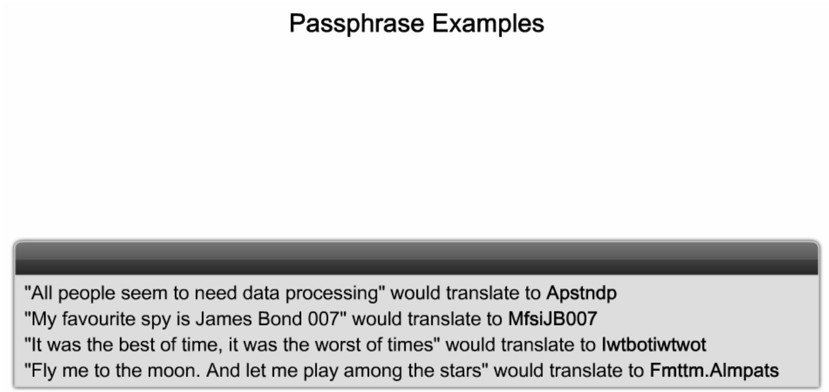
Applying Cisco IOS Security Features to Routers

Steps to safeguard a router:

Step 1. Manage router security
Step 2. Secure remote administrative access to routers
Step 3. Logging router activity
Step 4. Secure vulnerable router services and interfaces
Step 5. Secure routing protocols
Step 6. Control and filter network traffic

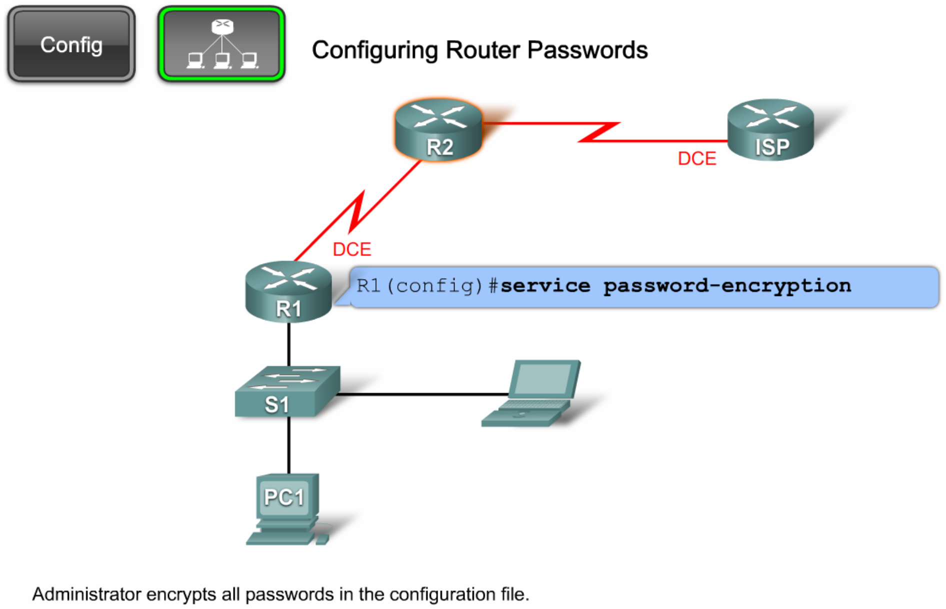
Configure Basic Router Security

- Describe the basic security measures needed to secure Cisco routers



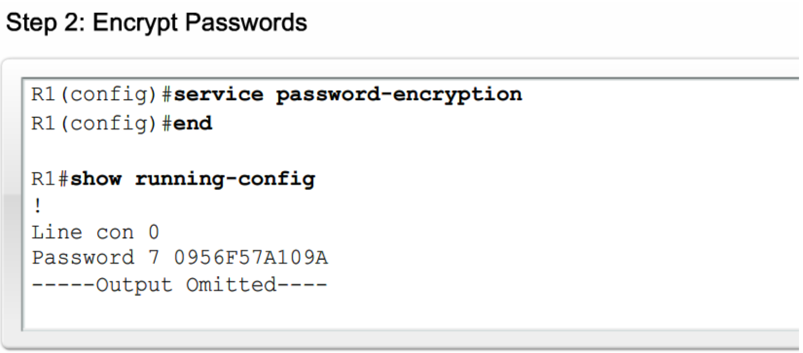
Passphrase Examples

"All people seem to need data processing" would translate to **Apstndp**
"My favourite spy is James Bond 007" would translate to **MfsiJB007**
"It was the best of time, it was the worst of times" would translate to **Iwtbotiwtwot**
"Fly me to the moon. And let me play among the stars" would translate to **Fmttm.Almpats**



```
R1(config)#service password-encryption
```

Administrator encrypts all passwords in the configuration file.



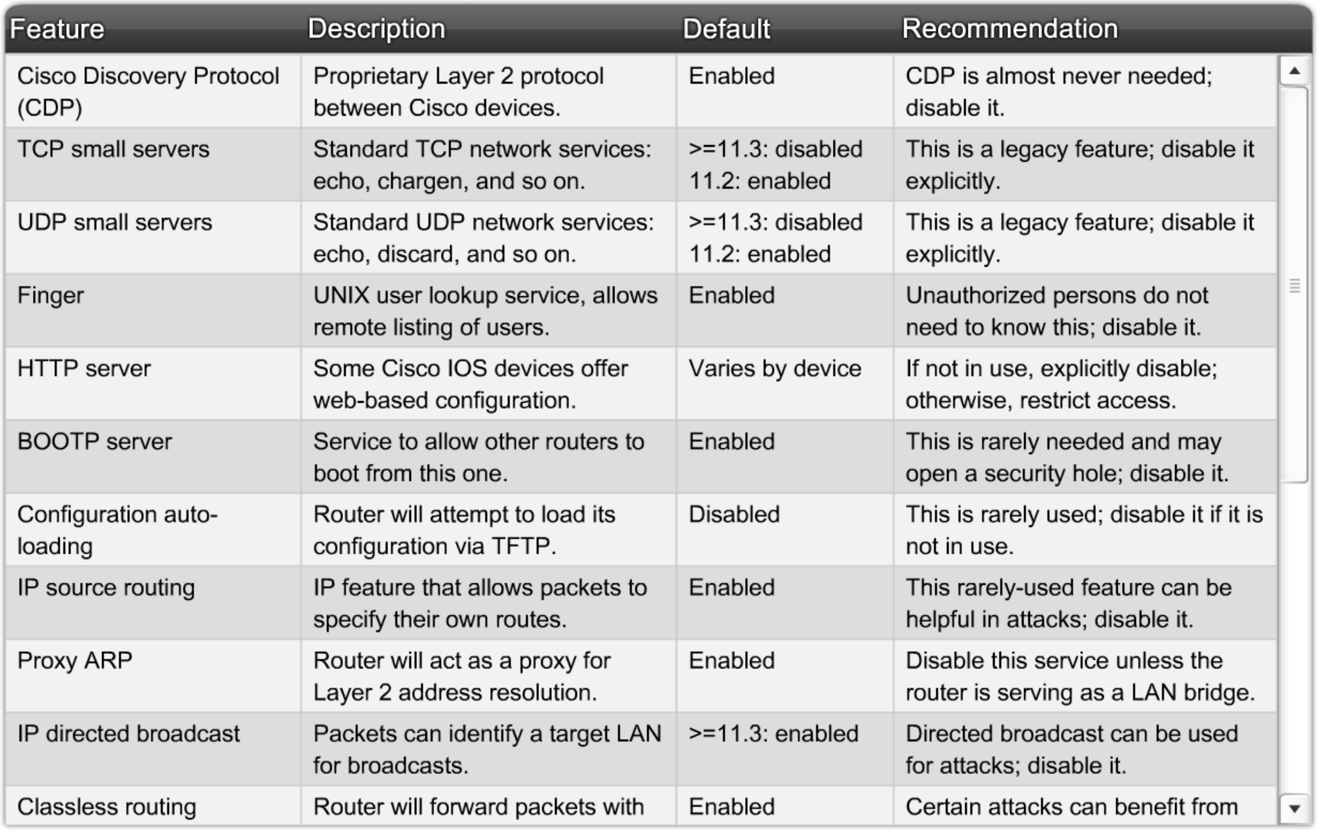
Step 2: Encrypt Passwords

```
R1(config)#service password-encryption
R1(config)#end

R1#show running-config
!
Line con 0
Password 7 0956F57A109A
-----Output Omitted----
```

Explain How to Disable Unused Cisco Router Network Services and Interfaces

- Describe the router services and interfaces that are vulnerable to network attack

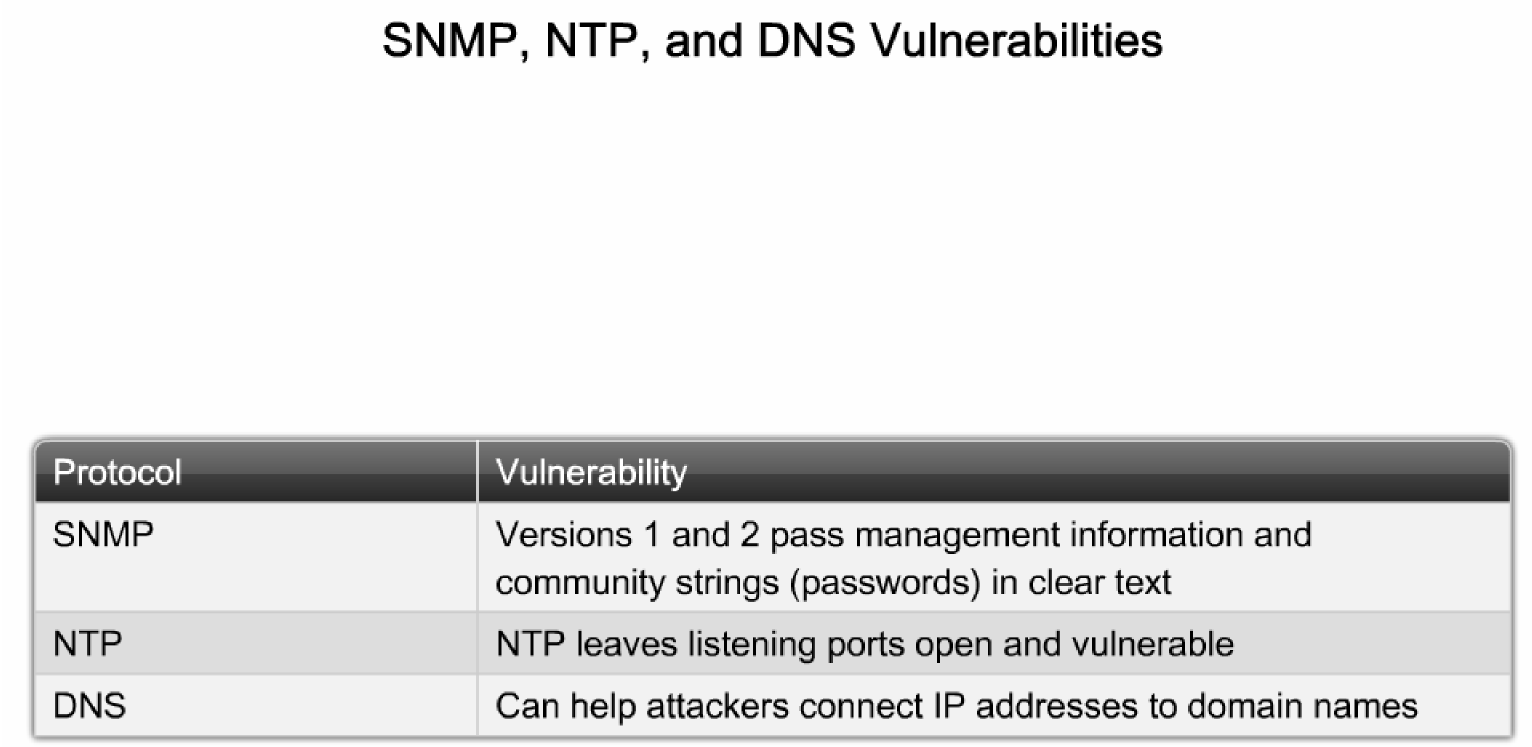
Vulnerable Router Services



Feature	Description	Default	Recommendation
Cisco Discovery Protocol (CDP)	Proprietary Layer 2 protocol between Cisco devices.	Enabled	CDP is almost never needed; disable it.
TCP small servers	Standard TCP network services: echo, chargen, and so on.	>=11.3: disabled 11.2: enabled	This is a legacy feature; disable it explicitly.
UDP small servers	Standard UDP network services: echo, discard, and so on.	>=11.3: disabled 11.2: enabled	This is a legacy feature; disable it explicitly.
Finger	UNIX user lookup service, allows remote listing of users.	Enabled	Unauthorized persons do not need to know this; disable it.
HTTP server	Some Cisco IOS devices offer web-based configuration.	Varies by device	If not in use, explicitly disable; otherwise, restrict access.
BOOTP server	Service to allow other routers to boot from this one.	Enabled	This is rarely needed and may open a security hole; disable it.
Configuration auto-loading	Router will attempt to load its configuration via TFTP.	Disabled	This is rarely used; disable it if it is not in use.
IP source routing	IP feature that allows packets to specify their own routes.	Enabled	This rarely-used feature can be helpful in attacks; disable it.
Proxy ARP	Router will act as a proxy for Layer 2 address resolution.	Enabled	Disable this service unless the router is serving as a LAN bridge.
IP directed broadcast	Packets can identify a target LAN for broadcasts.	>=11.3: enabled	Directed broadcast can be used for attacks; disable it.
Classless routing	Router will forward packets with	Enabled	Certain attacks can benefit from

Explain How to Disable Unused Cisco Router Network Services and Interfaces

- Explain the vulnerabilities posed by commonly configured management services



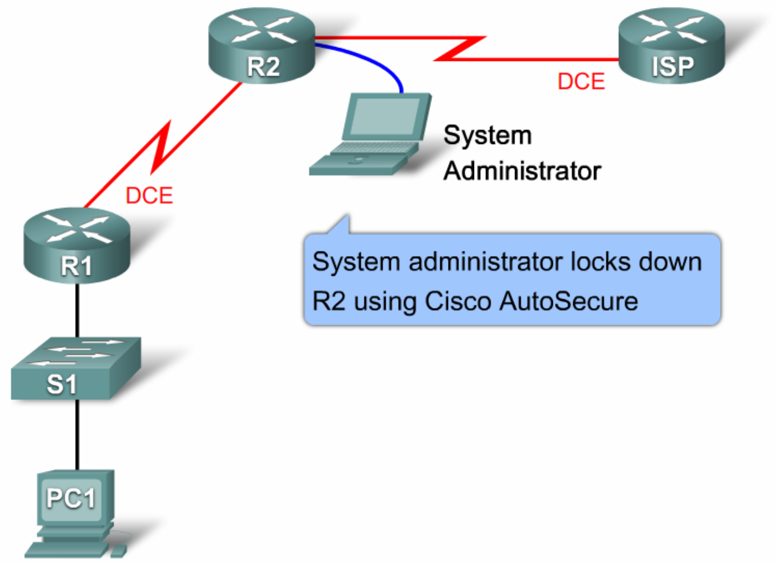
SNMP, NTP, and DNS Vulnerabilities

Protocol	Vulnerability
SNMP	Versions 1 and 2 pass management information and community strings (passwords) in clear text
NTP	NTP leaves listening ports open and vulnerable
DNS	Can help attackers connect IP addresses to domain names

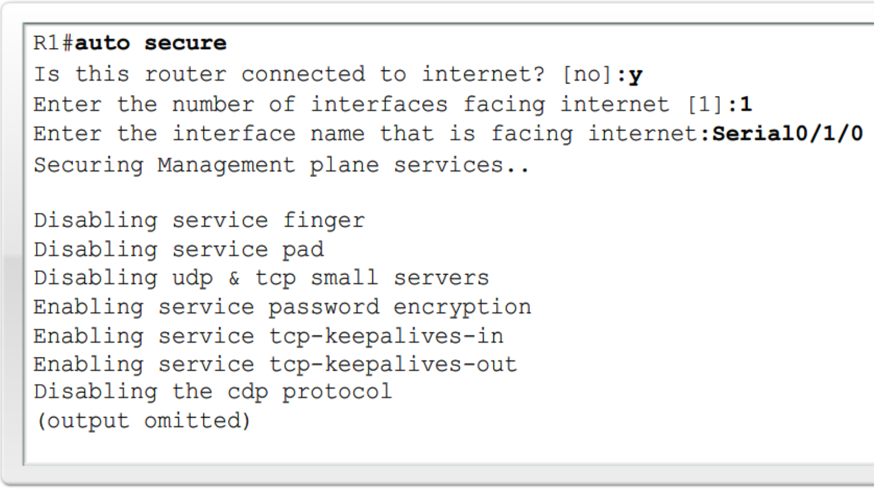
Explain How to Disable Unused Cisco Router Network Services and Interfaces

- Explain how to secure a router with the command-line interface (CLI) auto secure command

Locking Down Your Router with Cisco AutoSecure



System administrator locks down R2 using Cisco AutoSecure

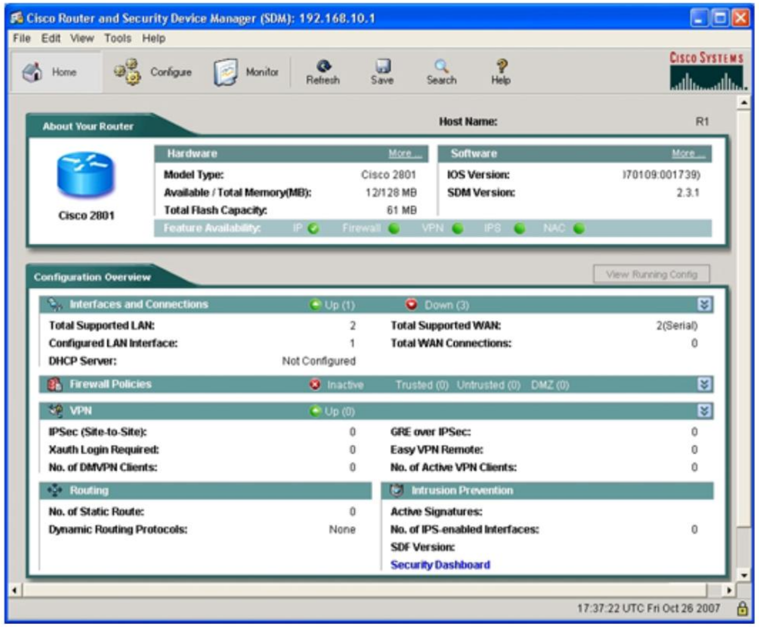


```
R1#auto secure
Is this router connected to internet? [no]:y
Enter the number of interfaces facing internet [1]:1
Enter the interface name that is facing internet:Serial0/1/0
Securing Management plane services..

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
(output omitted)
```

Explain How to Use Cisco SDM

- Provide an overview of Cisco SDM

What Is Cisco SDM?



Host Name: R1

Hardware

Model Type: Cisco 2801
Available / Total Memory(MB): 12/128 MB
Total Flash Capacity: 61 MB

Software

IOS Version:)70109:001739)
SDM Version: 2.3.1

Feature Availability: IP ● Firewall ● VPN ● IPS ● NAC ●

Interfaces and Connections ● Up (1) ● Down (3)

Total Supported LAN: 2
Configured LAN Interface: 1
DHCP Server: Not Configured
Total Supported WAN: 2(Serial)
Total WAN Connections: 0

Firewall Policies ● Inactive Trusted (0) Untrusted (0) DMZ (0)

VPN ● Up (0)

IPSec (Site-to-Site): 0
Xauth Login Required: 0
No. of DMVPN Clients: 0
GRE over IPSec: 0
Easy VPN Remote: 0
No. of Active VPN Clients: 0

Routing

No. of Static Route: 0
Dynamic Routing Protocols: None

Intrusion Prevention

Active Signatures:
No. of IPS-enabled Interfaces: 0
SDF Version:

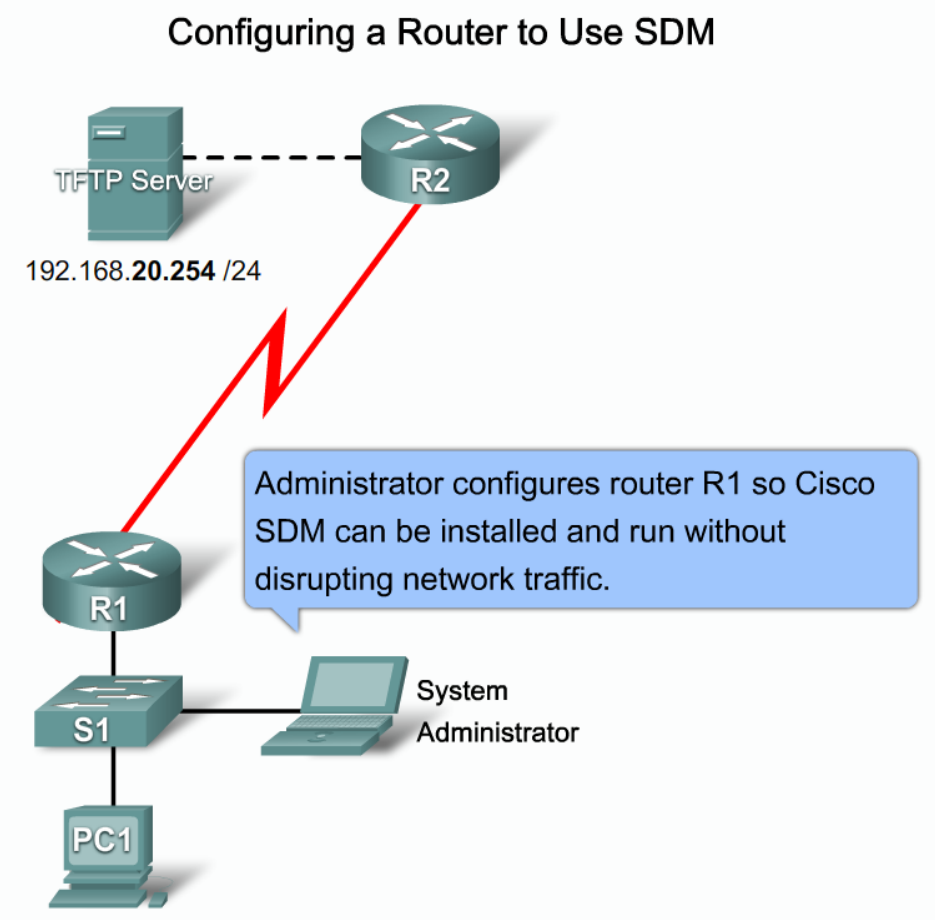
17:37:22 UTC Fri Oct 26 2007

Cisco SDM Features

- Embedded web-based management tool
- Intelligent wizards
- Tools for more advanced users
  - ACL
  - VPN crypto map editor
  - Cisco IOS CLI preview

Explain How to Use Cisco SDM

- Explain the steps to configure a router to use Cisco SDM

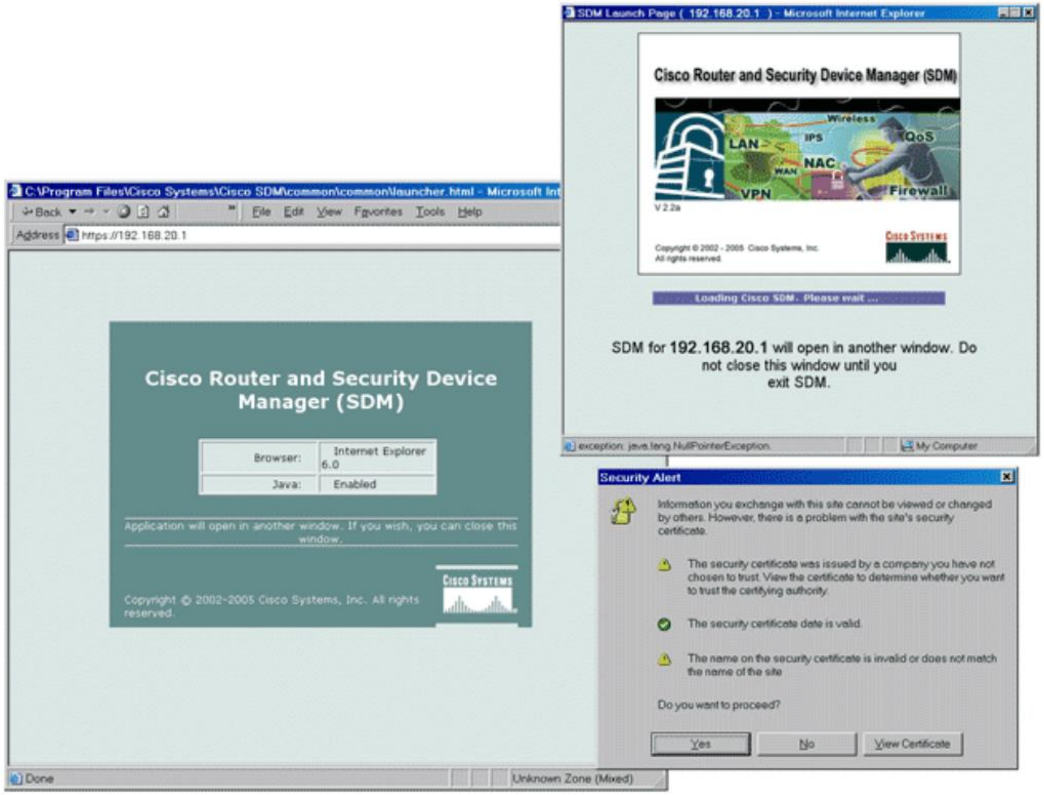

Configuring a Router to Use SDM

Administrator configures router R1 so Cisco SDM can be installed and run without disrupting network traffic.

Explain How to Use Cisco SDM

- Explain the steps you follow to start SDM

Starting Cisco SDM



C:\Program Files\Cisco Systems\Cisco SDM\common\common\launcher.html - Microsoft Int
Back
File
Edit
View
Favorites
Tools
Help
Address
https://192.168.20.1

Cisco Router and Security Device Manager (SDM)

Browser:	Internet Explorer 6.0
Java:	Enabled

Application will open in another window. If you wish, you can close this window.

Copyright © 2002-2005 Cisco Systems, Inc. All rights reserved.

Cisco Systems
Done
Unknown Zone (Mixed)
SDM Launch Page (192.168.20.1) - Microsoft Internet Explorer

Cisco Router and Security Device Manager (SDM)

Copyright © 2002 - 2005 Cisco Systems, Inc.
All rights reserved.

Loading Cisco SDM. Please wait ...

SDM for 192.168.20.1 will open in another window. Do not close this window until you exit SDM.

exception: java.lang.NullPointerException.

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

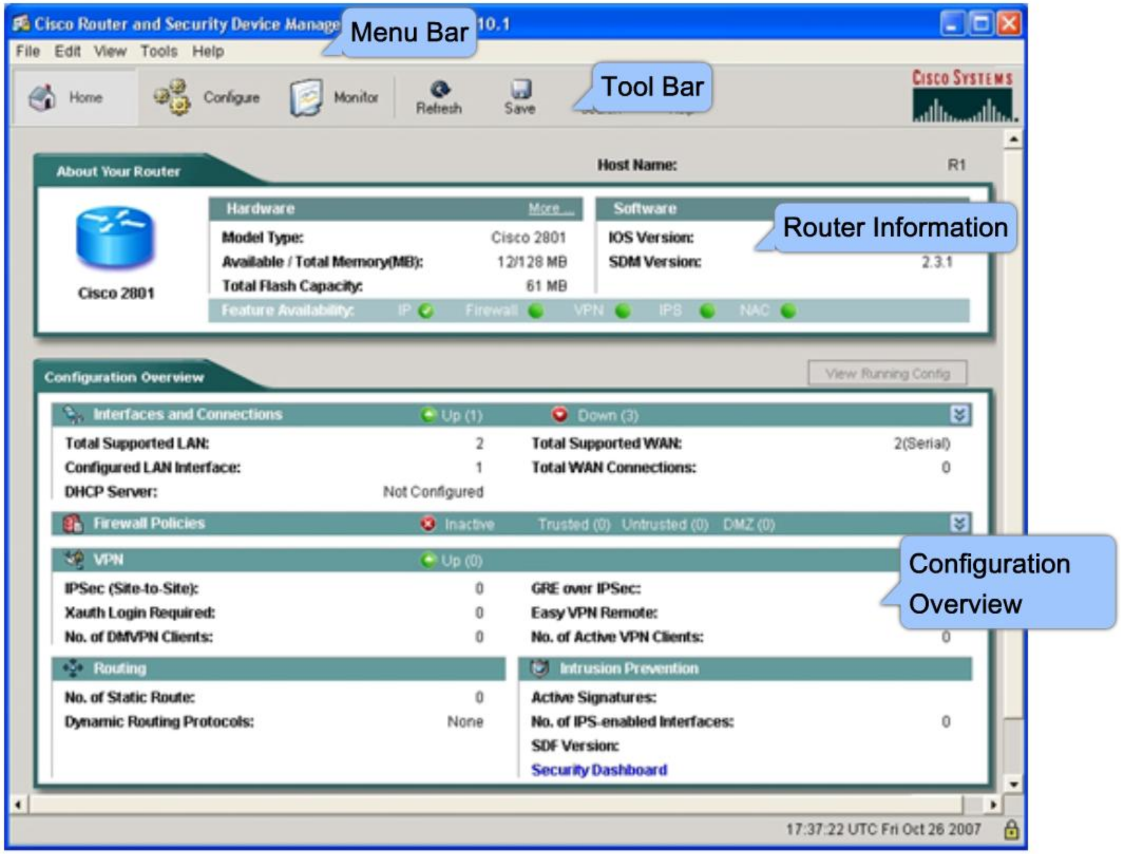
The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Explain How to Use Cisco SDM

- Describe the Cisco SDM Interface

Cisco SDM Home Page Overview



Cisco Router and Security Device Manage 10.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Cisco Systems

Menu Bar

Tool Bar

About Your Router

Host Name: R1

Cisco 2801

Hardware More...

Model Type: Cisco 2801

Available / Total Memory(MB): 12/128 MB

Total Flash Capacity: 61 MB

Software

IOS Version:

SDM Version: 2.3.1

Feature Availability: IP ● Firewall ● VPN ● IPS ● NAC ●

Router Information

Configuration Overview

Interfaces and Connections ● Up (1) ● Down (3)

Total Supported LAN: 2

Configured LAN Interface: 1

DHCP Server: Not Configured

Total Supported WAN: 2(Serial)

Total WAN Connections: 0

Firewall Policies ● Inactive Trusted (0) Untrusted (0) DMZ (0)

VPN ● Up (0)

IPSec (Site-to-Site): 0

Xauth Login Required: 0

No. of DMVPN Clients: 0

GRE over IPSec:

Easy VPN Remote:

No. of Active VPN Clients: 0

Configuration Overview

Routing

No. of Static Route: 0

Dynamic Routing Protocols: None

Intrusion Prevention

Active Signatures:

No. of IPS-enabled Interfaces: 0

SDF Version:

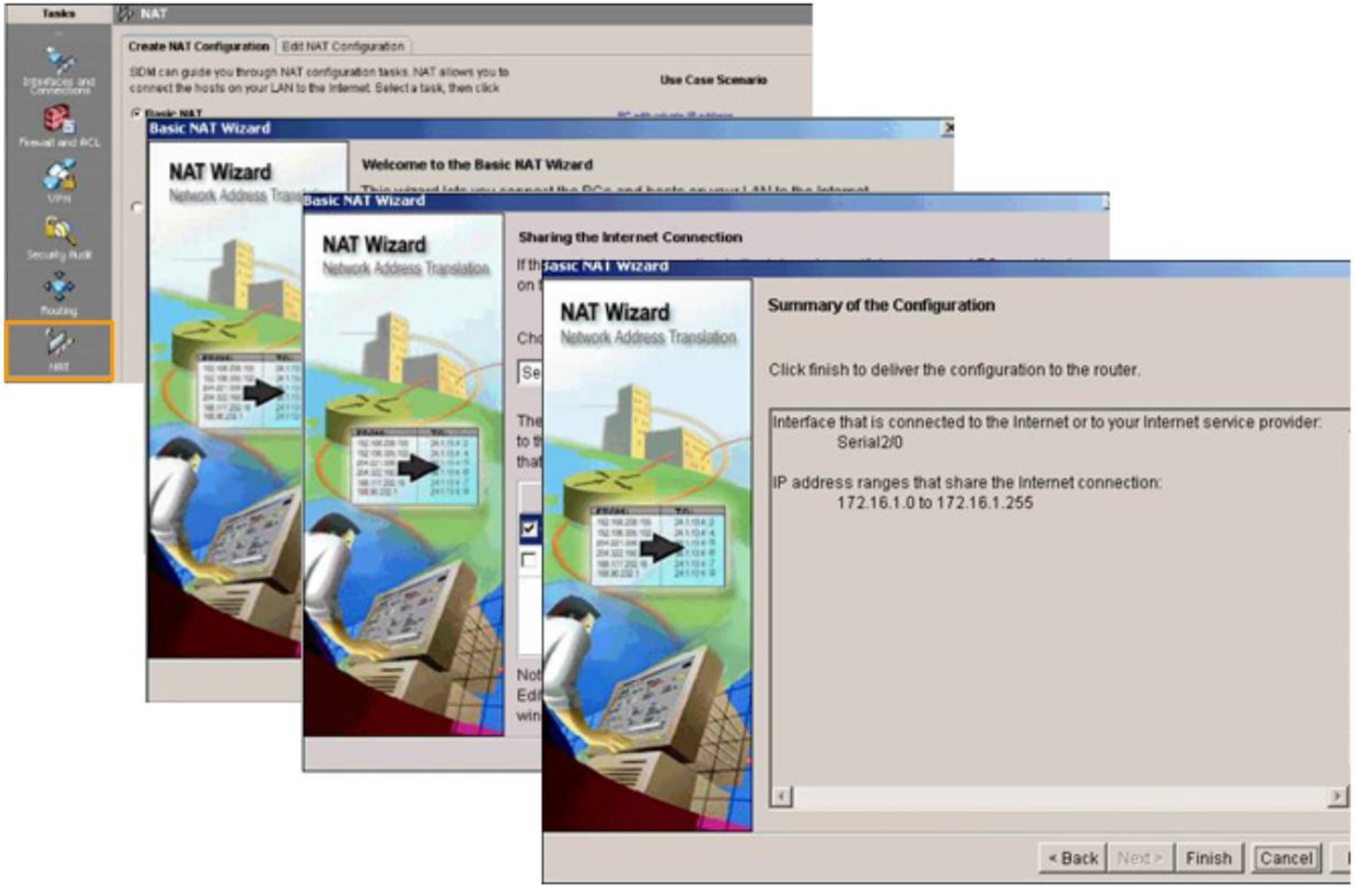
Security Dashboard

17:37:22 UTC Fri Oct 26 2007

Explain How to Use Cisco SDM

- Describe the commonly used Cisco SDM wizards

Cisco SDM Wizards



SDM can guide you through NAT configuration tasks. NAT allows you to connect the hosts on your LAN to the Internet. Select a task, then click

Welcome to the Basic NAT Wizard

Sharing the Internet Connection

Summary of the Configuration

Click finish to deliver the configuration to the router.

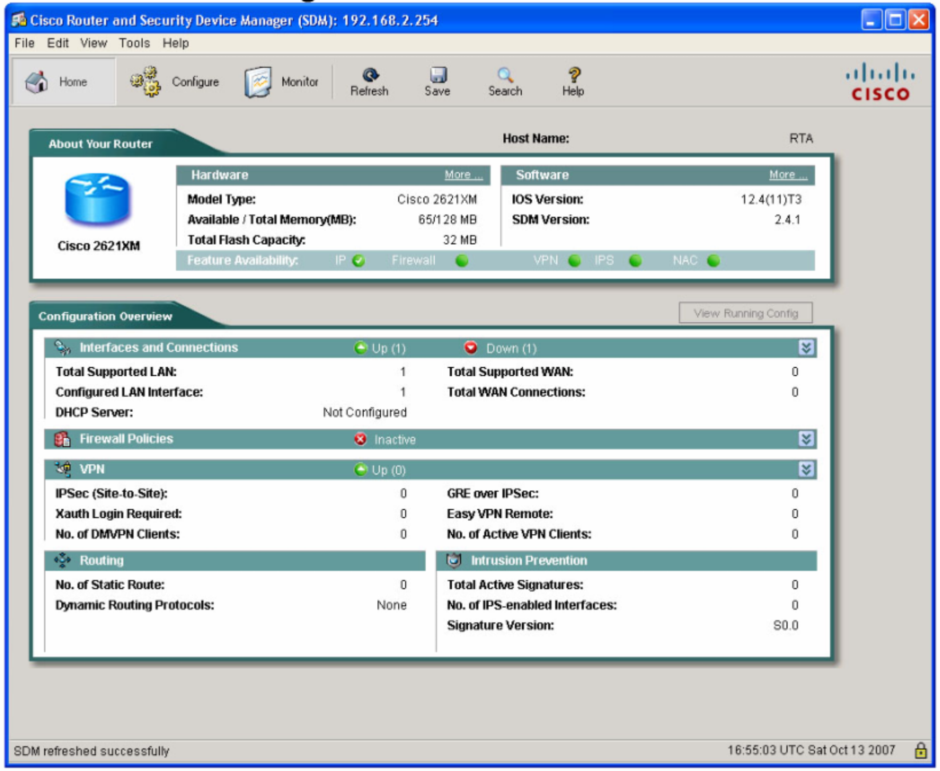
Interface that is connected to the Internet or to your Internet service provider:
Serial2/0

IP address ranges that share the Internet connection:
172.16.1.0 to 172.16.1.255

Explain How to Use Cisco SDM

- Explain how to use Cisco SDM for locking down your router

Locking Down a Router with Cisco SDM



Cisco Router and Security Device Manager (SDM): 192.168.2.254
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO

About Your Router

Host Name: RTA

Cisco 2621XM

Hardware — More ...

Model Type: Cisco 2621XM

Available / Total Memory(MB): 65/128 MB

Total Flash Capacity: 32 MB

Software — More ...

IOS Version: 12.4(11)T3

SDM Version: 2.4.1

Feature Availability: IP ● Firewall ● VPN ● IPS ● NAC ●

Configuration Overview

Interfaces and Connections — Up (1) — Down (1)

Total Supported LAN: 1

Configured LAN Interface: 1

DHCP Server: Not Configured

Total Supported WAN: 0

Total WAN Connections: 0

Firewall Policies — Inactive

VPN — Up (0)

IPSec (Site-to-Site): 0

Xauth Login Required: 0

No. of DMVPN Clients: 0

GRE over IPSec: 0

Easy VPN Remote: 0

No. of Active VPN Clients: 0

Routing

No. of Static Route: 0

Dynamic Routing Protocols: None

Intrusion Prevention

Total Active Signatures: 0

No. of IPS-enabled Interfaces: 0

Signature Version: S0.0

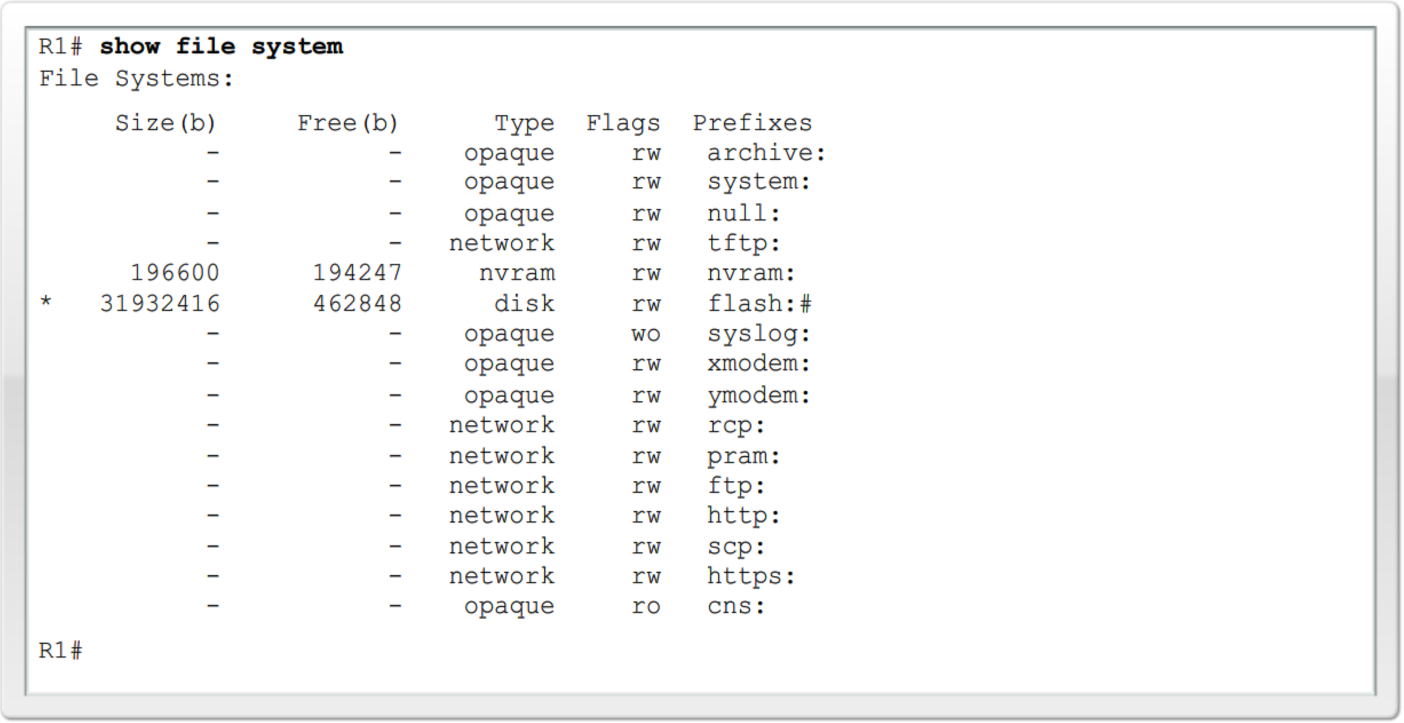
SDM refreshed successfully

16:55:03 UTC Sat Oct 13 2007

Manage Cisco IOS Devices

- Describe the file systems used by a Cisco router

File Systems

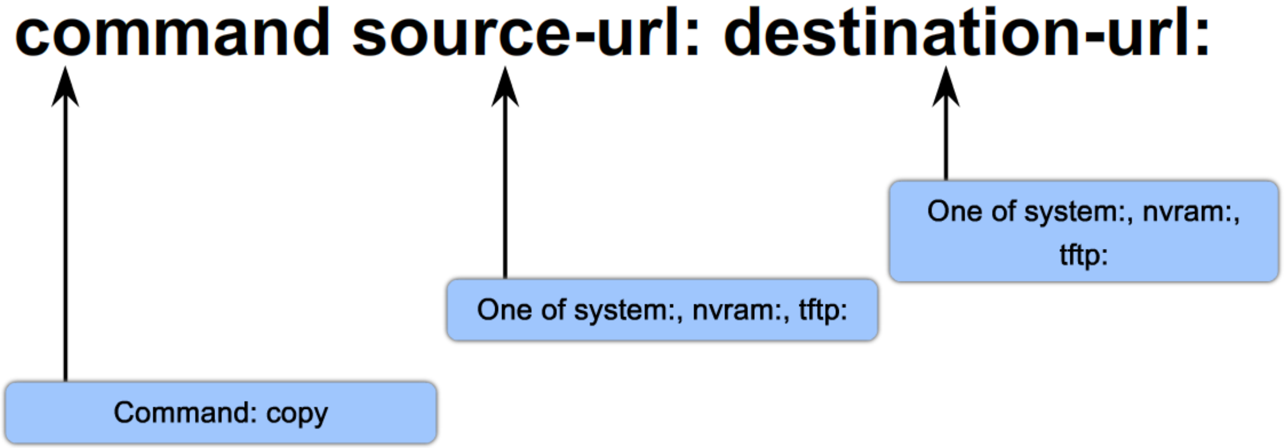


```
R1# show file system
File Systems:

     Size(b)       Free(b)      Type  Flags  Prefixes
           -             -    opaque     rw   archive:
           -             -    opaque     rw   system:
           -             -    opaque     rw   null:
           -             -   network     rw   tftp:
      196600        194247     nvram     rw   nvram:
*   31932416        462848      disk     rw   flash:#
           -             -    opaque     wo   syslog:
           -             -    opaque     rw   xmodem:
           -             -    opaque     rw   ymodem:
           -             -   network     rw   rcp:
           -             -   network     rw   pram:
           -             -   network     rw   ftp:
           -             -   network     rw   http:
           -             -   network     rw   scp:
           -             -   network     rw   https:
           -             -    opaque     ro   cns:

R1#
```

Manage Cisco IOS Devices

- Describe how to backup and upgrade a Cisco IOS image

Commands for Managing Configuration Files



command source-url: destination-url:

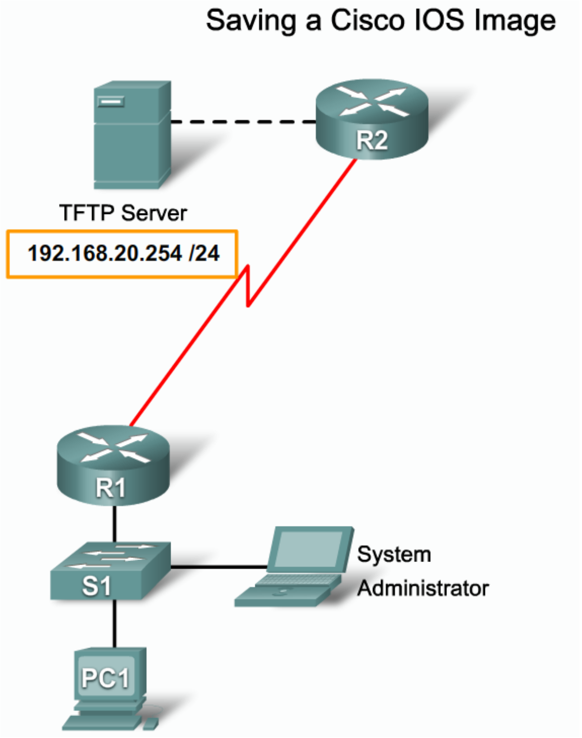
Command: copy

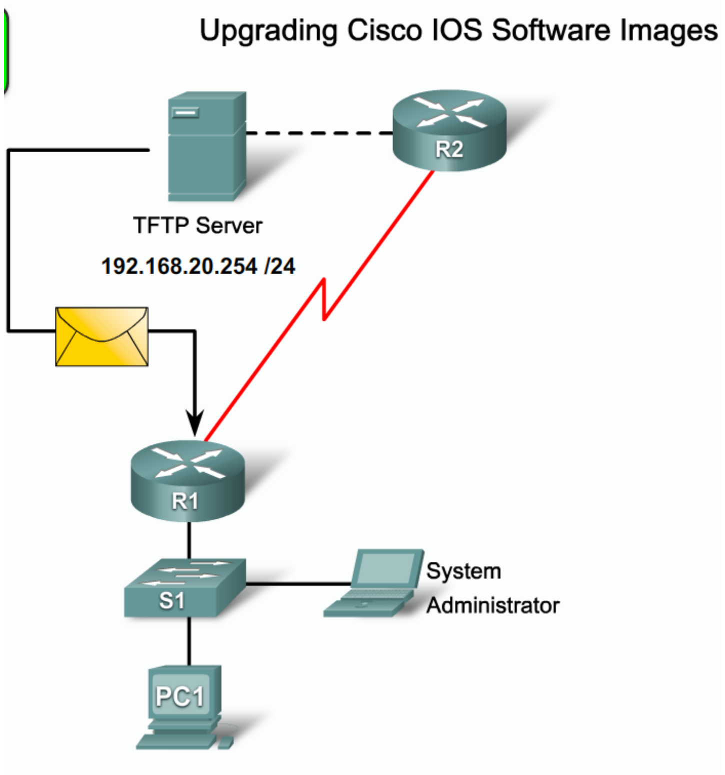
One of system:, nvram:, tftp:

One of system:, nvram:, tftp:

Manage Cisco IOS Devices

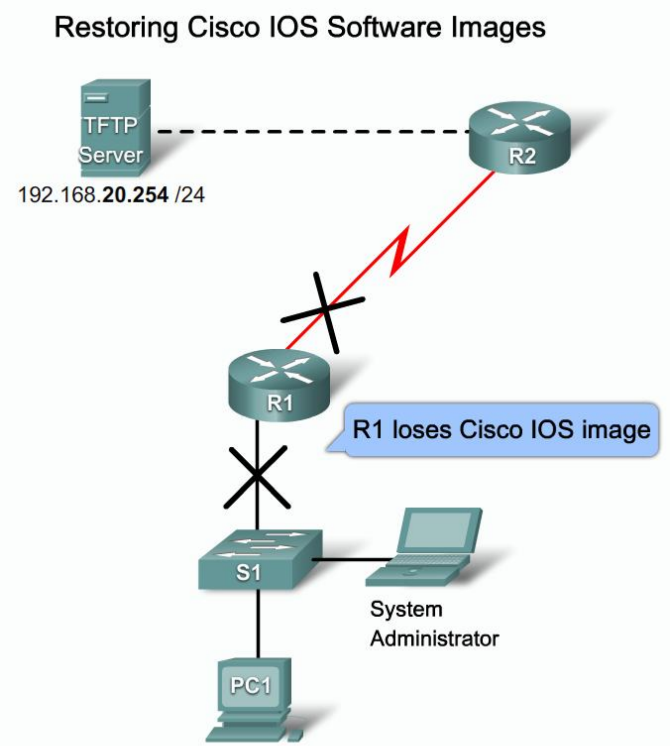
- Explain how to back up and upgrade Cisco IOS software images using a network server

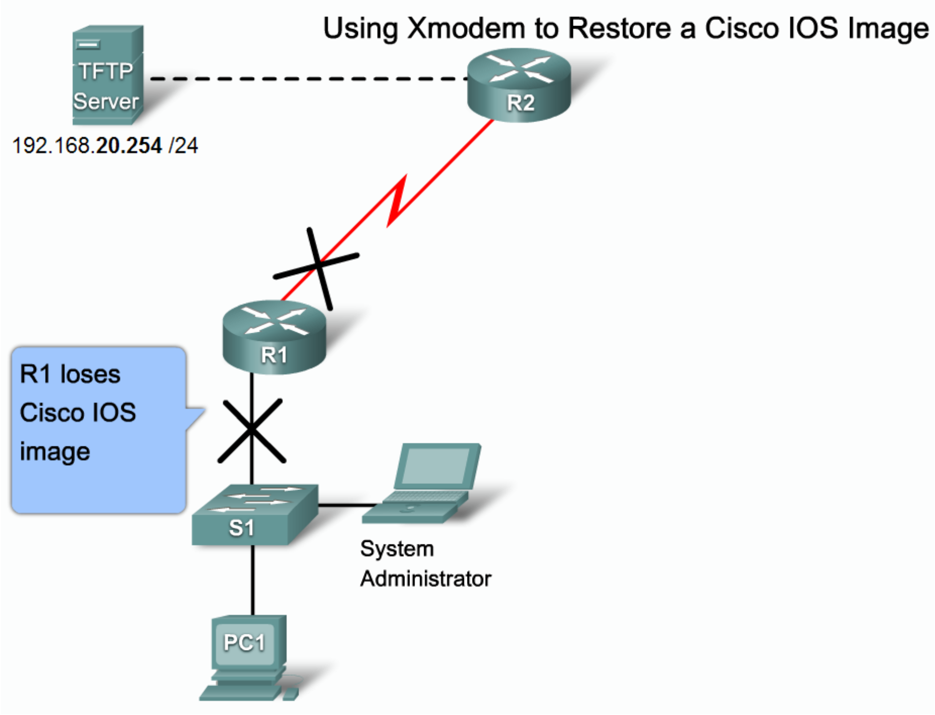




Manage Cisco IOS Devices

- Explain how to recover a Cisco IOS software image

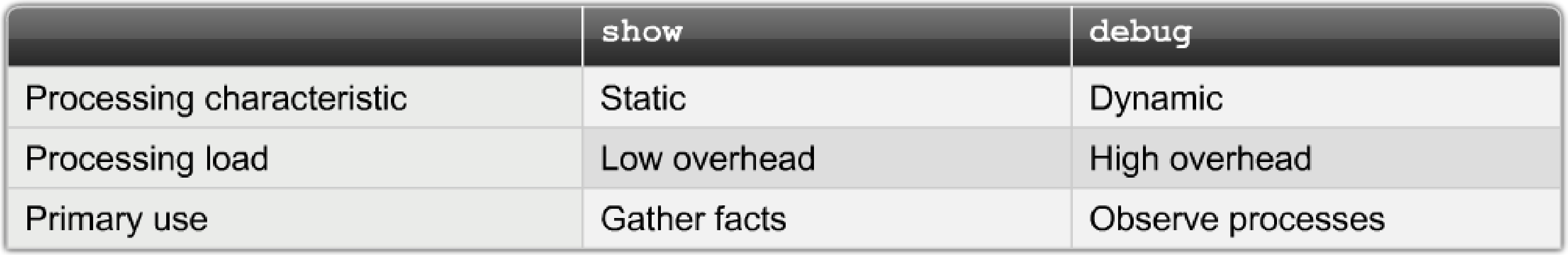




Manage Cisco IOS Devices

- Compare the use of the show and debug commands when troubleshooting Cisco router configurations

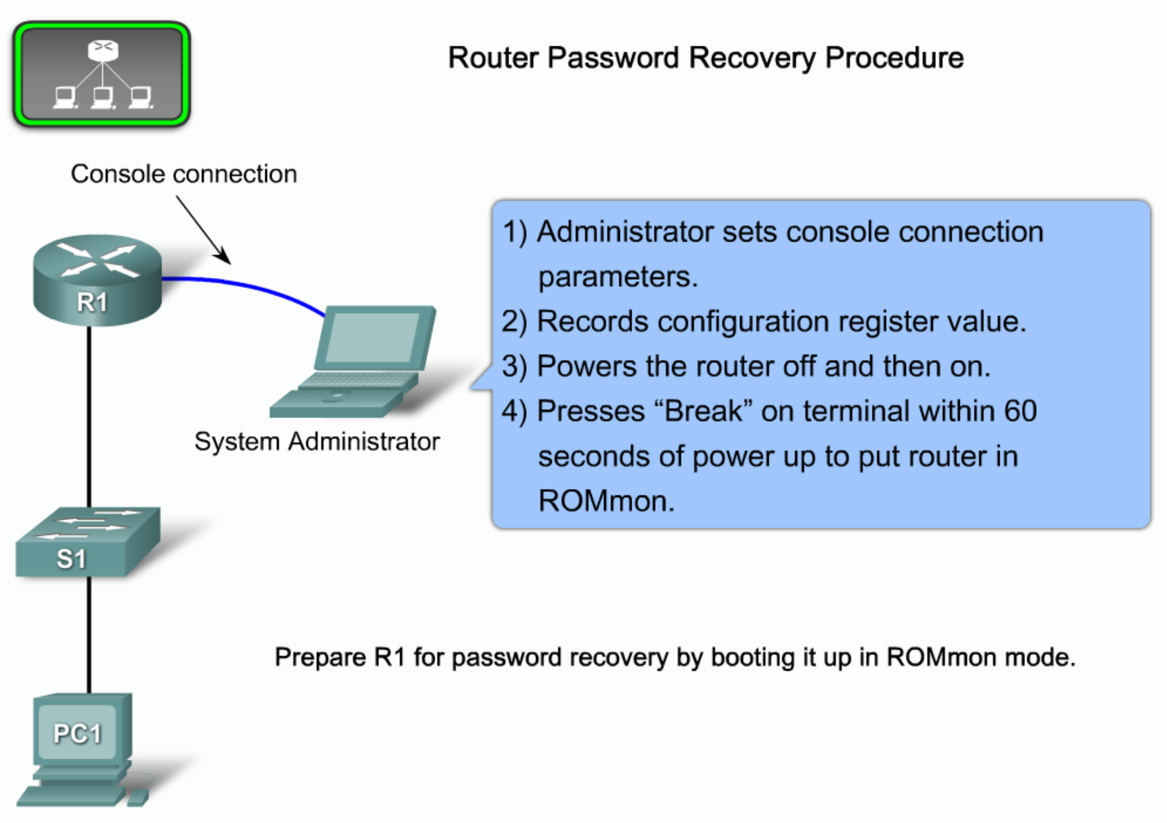
Cisco IOS Troubleshooting Commands



	show	debug
Processing characteristic	Static	Dynamic
Processing load	Low overhead	High overhead
Primary use	Gather facts	Observe processes

Manage Cisco IOS Devices

- Explain how to recover the enable password and the enable secret passwords



Router Password Recovery Procedure

1) Administrator sets console connection parameters.
2) Records configuration register value.
3) Powers the router off and then on.
4) Presses “Break” on terminal within 60 seconds of power up to put router in ROMmon.

Prepare R1 for password recovery by booting it up in ROMmon mode.

Summary

- Security Threats to an Enterprise network include:
  - –Unstructured threats
  - –Structured threats
  - –External threats
  - –Internal threats
- Methods to lessen security threats consist of:
  - –Device hardening
  - –Use of antivirus software
  - –Firewalls
  - –Download security updates

Summary

- Basic router security involves the following:
  - –Physical security
  - –Update and backup IOS
  - –Backup configuration files
  - –Password configuration
  - –Logging router activity
- Disable unused router interfaces & services to minimize their exploitation by intruders
- Cisco SDM
  - –A web based management tool for configuring security measures on Cisco routers

Summary

- Cisco IOS Integrated File System (IFS)
  - –Allows for the creation, navigation & manipulation of directories on a cisco device